A VPN Security Solution for Connectivity over Insecure Network Channels: A novel study.

Attlee M. Gamundani[1], Julia N. Nambili[2], Mercy Bere[3]
[1,2,3](Department of Computer Science, Polytechnic of Namibia, Namibia)

ABSTRACT : *Remote access is one of the prevalent business trends in today's ubiquitous environments. The ease of access to internet connectivity has given birth to user flexibility on file access, where access to internal private networks over the internet (which is by nature insecure) is being done from homes, hotels, airports or from other external network access points. This has a tendency of exposing sensitive files or data to intruders like man in the middle attack, denial of service and many other security threats. A VPN (Virtual Private Network) promises a secure private network through a shared public insecure infrastructure like the internet. VPN technology has proven its value for delivering new services while at the same time offering a security layer. In this research, we are going to simulate scalability of VPN connectivity over insecure channels using Packet Tracer. The simulation results though limited in scope will prove the viability of employing VPN technology. The need to address security concerns for organizations is highly meet with VPN implementations. This research employed the case study approach, where Ministry of Justice in Namibia was the main focal point of attention; therefore the scope of this research was limited to that domain.*

Keywords - *Access, Private, Public, Security, VPN*

I. INTRODUCTION

VPN provides an encrypted and secure connection "tunnel" path from a user's machine to its destination through the public internet (1). The internet has become a popular, low cost backbone infrastructure. Its universal reach has led many companies to consider constructing a secure VPN over the public internet (1). A private network creates a notion of computers and network resources that belong to a single dedicated user or organization. The pool of computers and network resources, though they make use of the public network facilities (i.e. ISP networks), assume independence and total ownership of the resources (8). VPN is one method for interconnecting multiple sites belonging to the same organization using an Internet Service Provider (ISP) backbone network in place of a dedicated line (23). The use of public telecommunication infrastructure reduces operational costs while enhancing the security requirements through the security protocols and procedures (13). VPN achieves implementation of a private network on top of the internet technology infrastructure using modern switching or routing hardware capabilities, encryption, authentication, packet tunneling and firewalls (22). Such robustness renders VPN a scalable technology that has the potential to solve many of business networking problems (1).

II. CASE STUDY SETTING

A. Overview of Ministry of Justice(MoJ)

Ministry of Justice (herein henceforth referred to as MoJ) is one of the main and large important ministries in Namibia responsible for upholding the law, rules and regulations in the country. It is represented across and in all regions of the country with more than 30 offices in different towns. The most important constituents and representatives of the ministry are magistrate, high and supreme courts. Information collected and processed at the various stations (remote offices) are of high importance and mostly confidential. Despite this, the connectivity between the remote offices is accomplished by the use of dedicated lease lines, which is not only unreliable and inconvenient to the systems administrators but also very costly. Due to the high cost of lease lines, MoJ cannot afford to constantly have the remote office connected to the head office. Data gathering and information sharing is a challenge as each office is treated as a standalone station.

The biggest challenge that ignited this research is the enormous strain on both the administration staff as well as all operational staff in the regions, caused by the prevailing ICT setups. As presented by (16), some information is critical to the operation of such organizations as ministry of justice in any country, however, the disclosure of such information to unauthorized people will

compromise personal safety and the integrity of the system.

The Ministry needs a solution that would enable the sharing and accessing of data in a secure and efficient manner. It is against this background that this study is being undertaken to explore the possibility of implementing the Virtual Private Network (VPN) for the Ministry of Justice's immediate needs.

B. MoJ Operations without Virtual Private Network (VPN)

MoJ have more than 80 servers deployed to regional offices. Each regional office has more than 1 server. With the rolling out of the Namibian Court integrated System (NAMCIS), a system that does the administration of court cases, more servers had to be deployed to the regional offices. Two servers are in each regional office, each office is a standalone office, and there is no integration with other offices. One of the servers act as the Domain Controller (DC) and the other one only run NAMCIS. Services running on the DC are the printing servers, file server, proxy server and Active Directory (AD) services. User applications are installed on the client machines and the setups are saved on the Domain Controller. NAMCIS servers at MoJ offices are independent of each other. The aim of NAMCIS is to create an information database that would be available at all regional offices in real time. The purpose is to ensure transparency within the administration of justice in Namibia.

The bandwidth between regional offices is not sufficient for replications. This is a challenge to court staff as at times data need to be captured manually more than once in scenarios where a case is transferred to a different region. For most regional offices, the servers are housed in the store room, full of documents hence poor ventilation. This clearly explains why MoJ will require a solution that will best suit the prevailing conditions without straining the resources at their disposal.

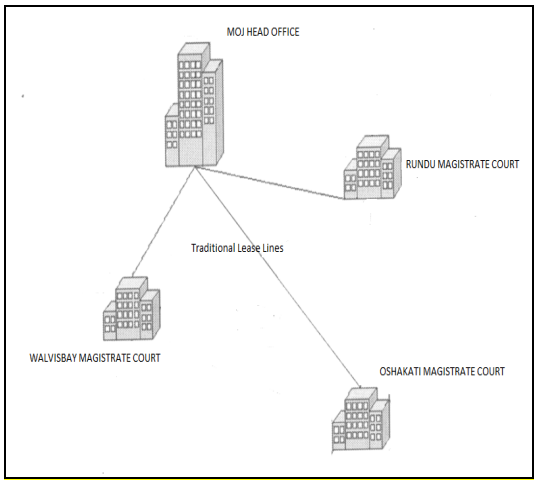

Figure 1: **Traditional Lease Lines (MoJ)**

The above figure 1 demonstrates the current spatial office distribution. Remote offices are connected to each other and the head office with dedicated lease lines.

Information sharing is a big challenge especially for offices outside Windhoek. Internal communication to occur they have to make use of courier services to regional offices most likely on a daily basis due to the lack of reliable email and internet services. Documents have to be printed, while larger data are burnt on CDs or DVDs. This is an expensive, time consuming and security risk practice. With implementation of VPN, MoJ will be moving closer towards a paperless, secure and ecofriendly environment.

Preservation of correct and adequate data at MoJ is of paramount importance to the administration of Justice in Namibia. Data captured in courts are customarily sensitive and rather confidential. It is the duty of the IT division to safeguard against all kind of data threats. As illustrated in (20), the Ministry of Justice of Georgia's IT department is responsible for the provision of electronic services and data sharing security. Alteration or deletion of data for unjust reason would jeopardize the just outcome of cases. It is important that the data are not only accurate but also available when required. The IT division is also tasked with the authentication responsibility, which guard against unauthorized access to information.

Currently, data is only available when the users are in their respective offices or regional offices. The users copy the documents they need to work on, away from the office, to their laptops as they cannot access the shared drive from anywhere else other than MoJ office buildings. There are currently no remote access users. This is a challenge as MoJ users work outside the office and have to put in long hours in office to do their chores efficiently. Remote Access would be ideal for MoJ staff especially the justice administration staff. These users travel a lot; they do a lot of research and the need to access information from the comfort of their remote sites is quite key.

Ministry of Justice is a crucial department of the Namibian government entrusted with law enforcement and regulation. However, the house faces challenges of network accessibility and security. As a result, this paper proposes implementing a Virtual Private Network; which is believed to offer the functionalities that realise the accessibility and security needs at MoJ.

II. VPN Overview

A. Overview

Virtual Private Network is defined as a network that uses a public network such as the Internet as a backbone to connect two or more private networks (1). The VPN encrypts and encapsulates each IP (Internet Protocol) packet before passing it through a tunnel (13), which is ideal for extranet connections. The VPN also uses the authentication information to check that the original data has not been corrupted during transmission, ensuring the integrity of the data (2, 3, 4, 5, 6, 7, 8, 9, and 10).

VPNs using the Internet have the potential to solve many of the business networking problems (1). A VPN uses the Internet infrastructure to interconnect sites and provide connectivity for remote dial-up users at competitive options. The wide coverage offered by the Internet eliminates the need for private leased lines and modem pools, this ultimately has cost saving effects (18).

B. Benefits of VPN

One of the most competing advantages of VPN is the cost reduction (1) (14). While VPN offers cost saving facilities, it also yields other advantages such as; reduced training requirements and equipment, increased flexibility and functional scalability (18).

Another important benefit of VPN is improved connectivity (19). MoJ can enjoy higher levels of connectivity through the Internet Service Provider arm, which are made possible through IP, Frame Relay or ATM infrastructure, often in conjunction with the internet (21). Above all, VPNs enable the delivery of broadband services that are capable of delivering emerging multimedia applications (17).

VPNs include comprehensive security policies that are another valuable commodity to organizations (15). With VPN, MoJ can be confident that their data remains private and that the transmissions are secure (17). The ability to prioritize traffic over a VPN ensures that the necessary bandwidth is available to mission critical applications when required (19).

C. Types of VPN connections

VPN connections can be achieved in two ways. The first method is by using Internet Protocol Security (IPSec) for authentication and encryption of services between endpoints. The second way is by using tunnelling mechanisms. Tunnelling means that the data being transmitted between end points is encapsulated inside another protocol. The following are some of the tunnelling protocols

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- Generic Routing Encapsulation (GRE)

There are two types of VPN connections, Remote Access VPN and a Site-to-site VPN. A Remote Access VPN connects employees of a company to the company intranet from home or when on the move. A site-to-site VPN connects geographically spaced out company intranets. Site-to-site VPN may also connect a company's intranet to a Business Partner's intranet. The table below summarises VPN features and characteristics.

Table1: VPN Features and Characteristics (24, 25)

VPN type	Features and characteristics
Remote Access	• Connect users to corporate network • Client server scheme • Internet Protocol Security • Use Secure Sockets Layer • Point to Point Tunnelling Protocol • Layer 2 Tunnelling Protocol
Site-to-site	• Connects networks • Hosts communicate through a VPN gateway • Internet Protocol Security • Generic Routing Encapsulation • Multi-Protocol Label Switching (MPLS)

To achieve full functionality of VPN connections, a mixture of the above components will ensure such a realisation. For the problem domain in this research paper, we recommend the site-to-site setup for certain applications, for the purposes of achieving full confidentiality capabilities. The major driver for such an option being the sensitive nature of data that may be shared among the responsible communicating branches in such an established connection. As depicted in Figure 2, a remote access VPN setup will enable access to emails and other communication requirements that may not involve exchange of sensitive data or documents.

III. Proposed Design of VPN Network

A. *Logical design for MoJ.*

In the Figure 2 below, the logical design of MoJ's VPN connectivity is depicted. The displayed logical layout is a simplified representation of the key pillars that will enable MPLS VPN connectivity via any ISP provider of choice the Ministry may opt for.

The MPLS/VPN architecture provides the capability to commission an IP network that delivers private network services over a shared infrastructure (13) at a competitive rate in comparison to other VPN dimensions such as SSL VPN; IPsec based VPN and IP VPN.

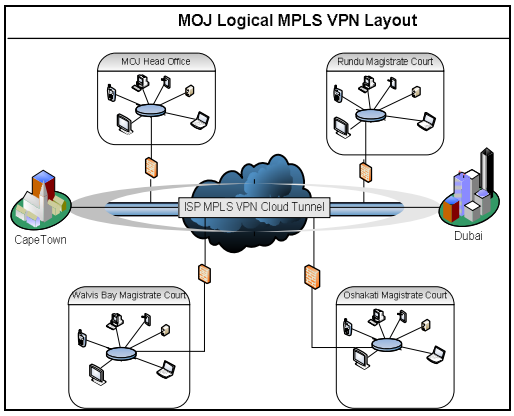

Figure 2 MoJ Envisaged VPN Design

IV. Simulation Design

A. *The Simulator: Packet Tracer*

For the simulation, an application Packet Tracer (PT) was used to simulate the network. PT is a network simulation program that allows experiments with network behaviors.

Packet Tracer is a protocol simulator developed at cisco systems. PT is a powerful and dynamic tool that displays the various protocols used in networking, either Real time or Simulation mode (26). This includes 2 protocols such as Ethernet and Point-Point-Protocol (PPP), layer 3 protocols such as IP, Internet Control Message Protocol (ICMP) and Address Resolution Protocol (ARP), and layer 4 protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)(27). PT remains a supplement to and not a replacement for experience with real life.

Due to functional limitations of PT, the software is recommended by cisco for learning purposes mainly; as such it will no replace real routers and switches (26). PT can be used to understand various concepts of networking with simulation. PT can be used to simulate the design and functionality of networks by facilitating troubleshooting and varied tests (26). Such a functionality offered by PT enables the building of a conceptual idea that will eventually materialize into practical implementations.

There are devices that are either at the client side (MoJ) as well as at the ISP side that are not represented in Packet Tracer, therefore cannot

be configured in Packet Tracer. The MPLS Internet Cloud for example is one of the setups that cannot be configured in packet tracer, to depict a full scale operation. The cloud is made up of many routers interlinking each other and a tunnel is created. A tunnel allows senders to encapsulate their data in IP packets and hide the routing and switching infrastructure of the internet (27). This is done to ensure data security against unwanted viewers or hackers.

B. The Simulation Layout in Packet Tracer.

Figure 3 represents the lab layout of the MoJ network in packet tracer. All the routers of MoJ as it shows are linked to the MPLS cloud router which is located at a service provider's network. Such a setup explains the advantages of implementing VPN. The monitoring of lines across the network layout is the responsibility of the ISP. Configurations done in this setup can be configured on the live network environment, though with added network equipment than simulated here. This kind of design is meant to help visualize the expected results in the live environment.

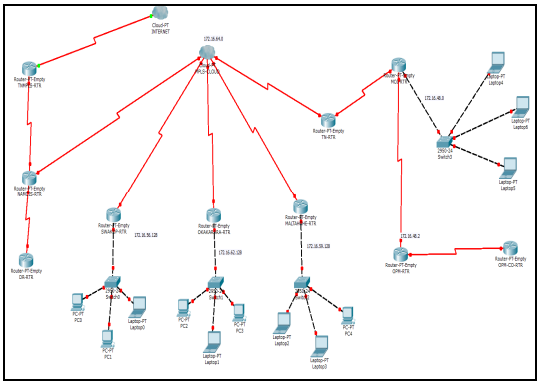

Figure 3: MoJ VPN Design in Packet Tracer

There are limitations in PT that affect the outcome results of VPN setups in PT. In a live environment, there are devices that cannot be configured or added on the design in PT by the client that have a great impact on the network results. These devices are only accessed and configured by the ISP. On the customer or client side, there is a device called Customer Edge (CE). The CE is located at the edge of the customer network and connects to the Provider Edge (PE) devices. The PE connects directly to customer network via CE devices. PE devices are aware of the PE based VPN but unaware of the VPN in CE based VPN as depicted in Figure 4, below.

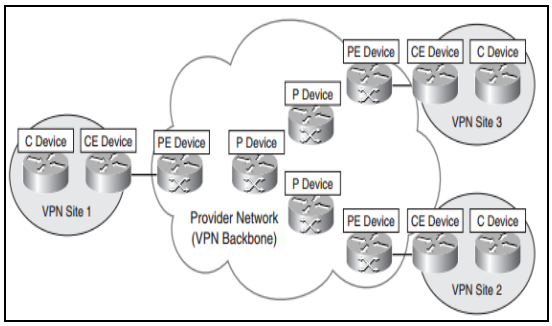

Figure 4: Customer and Provider network Devices (Cisco Labs)

Below is the simplest logical simulation of MoJ VPN setup. On Figure 5 below, only two branches are represented. Router 8 is representing the MPLS cloud and TN-RTR is the router at ISP connecting the MoJ network to the Cloud.

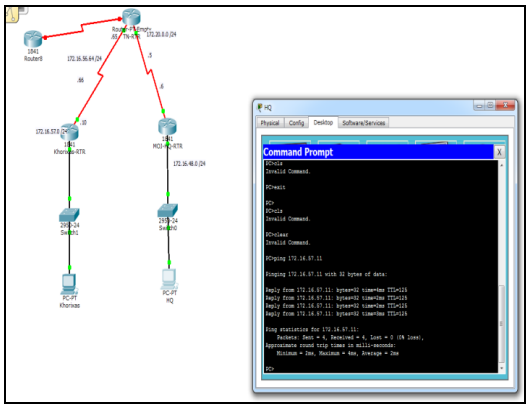

Figure 5: VPN Simulation in Packet Tracer

Connectivity between sites is tested by using a ping function from the site computers either to the Head office or to other remote offices. In the above insert, the Head Office is trying to establish connectivity to the computer in Khorixas and the ping results shows that there is no packet lost. The same results are expected vice versa.

A computer installed with VPN application and that can establish connectivity to the internet with authentication, will be able to establish connectivity to all configured devices on the MoJ network.

C. VPN Implementation Strategy

A phased approach to VPN planning and implementation as demonstrated by (12), promises to yield the key desired results. Figure 6, depicts a summarized representation generalized for any VPN planning and implementation project. The five cycle kit, if well employed will ensure the security concerns and application requirements are addressed holistically.

Considering the MoJ setup, during the identification of requirements phase, the nature of business need to be spelt out clearly for there are certain operations that may not be privy to the general public but forms the routine functional areas of any judiciary system. Such have to be defined guided by the security policies set thereof.

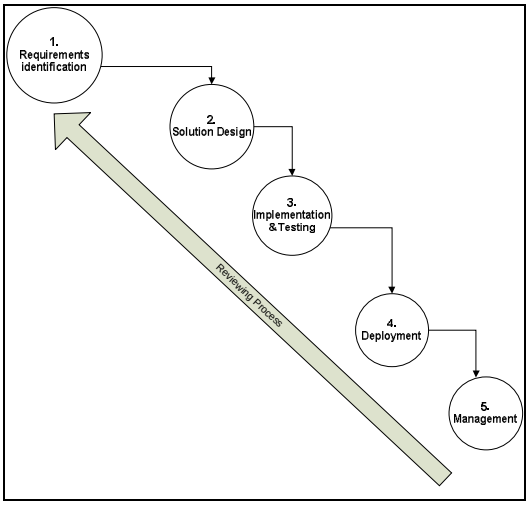

Figure 6: VPN Planning and Implementation Cycle (11)

VPN connections will allow users working at home or on the road to connect in a secure fashion to a remote server using the routing infrastructure provided by a public internetwork (such as the Internet)(22).

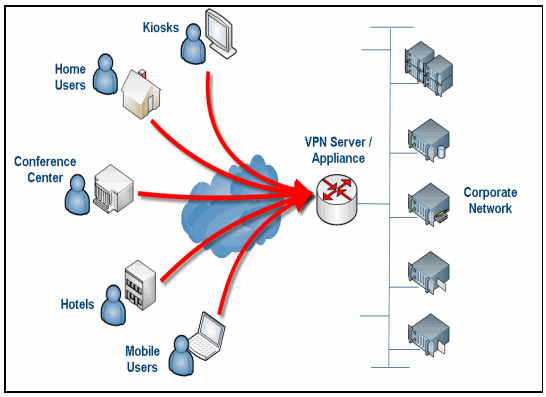

Figure 7: VPN Access to Corporate Network (ACA Networks, 2008)

Figure 7 shows the different locations from which employees can access the corporate network through VPN.

MoJ will use a VPN to communicate confidentially over a public network and to send voice, video or data, at a relatively secure level. It is also an excellent option for MoJ because of the remote workers and regional offices and partners that need to share data in a private manner. The communication channels between the regional offices and the head office is at the moment not adequate enough to allow for the transfer and access of data from all regional offices. The access and deployment to and of resources for regional offices is costing the ministry a lot of money. VPN replaces remote access servers and long distance dialup network connections. With VPN, the cost of maintaining servers tends to be less than other approaches because organizations can outsource the needed support from professional third-party service providers.

V. Conclusion and Discussion

This research mainly focused on how to provide connectivity at a cost effective way, while advancing security for such established connectivity. MPLS VPN connections are quite a scalable technology that embraces the existing IP protocol suites in availing a security layer for point to point connectivity spanning over a wide geographical locations.

Despite the limited simulation platforms utilised in this research, one of the key contributions that need to be emphasised is the functional capabilities of VPN technologies, that

organisations, whose operations demand high confidentiality and integrity attributes can make use of, if logically and systematically implemented following some of the guidelines summarised in this research.

Further research could be advanced in ensuring standardization of the VPN connection protocols that do not have properly spelt standards. Another area of focus within the domain of critical and sensitive applications, which could be explored, is the connectivity of WAN IP/VPN security as discussed by (16), proposing a solution through the Macedonian Telecommunications making use of the following hardware devices:-

- CISCO 2801 and CISCO 1841 routers and
- CISCO Catalyst 2950-24 LAN switches (16), for the Justin system in Columbia.

Generally security issues are not addressed by a single formula or dose, the need to systematically select the right mix of solutions that will address identified and unpredictable threats, is an art that need continual improvement in network security implementations.

VI. ACKNOWLEDGEMENTS

We acknowledge the key input from the esteemed staff members at Ministry of Justice (MoJ), who spared their time for appointments despite their busy diaries. We also appreciate the research atmosphere being created at Polytechnic of Namibia as it transforms into Namibia University of Science and Technology.

REFERENCES

[1] S.S. Riaz Ahamed and P. Rajamohan, Comprehensive performance analysis and special issues of Virtual Private Network strategies in the computer communication: A novel study. *International Journal of Engineering Science and Technology (IJEST), ISSN: 0975-5462, Vol 3. No.7, July 2011, 6040* (1)

[2] B. Gleeson et al, IP Based Virtual Private Networks, *RFC 2764*, February2000 (2)

[3] A. Nagarajan, Generic Requirements for Provider Provisioned Virtual Private Networks (PPVPN), *RFC3809*, June 2004 (3)

[4] L. Andersson and T. Madsen, Provider Provisioned Virtual Private Network (VPN) Terminology, *RFC4026*, March 2005 (4)

[5] E. Rosen & Y. Rekhter, BGP/MPLS VPNs, *RFC 2547*, March 1999 (5)

[6] Y. Rekhter et al., Address Allocation for Private Internets, *RFC 1918*, February 1996 (6)

[7] K. Muthukrishnan & A. Malis, A Core MPLS IP VPN Architecture, *RFC 2918*, September 2000 (7)

[8] A. Valencia et al., IP Based Virtual Private Networks, *RFC 2341*, May 1998 (8)

[9] Y.M. Chuang et al., Trading CDPD availability and voice blocking probability in cellular networks. *IEEE network, March- April 1998, pg. 48-52* (9)

[10] C. Metz, The latest in Virtual Private Networks: Part II. *IEEE, Internet Computing , pg. 60-65, 2004* (10)

[11] Y.R. Andu, VPN site to site packet tracer 5.3 Lab Version 1. *CCSI, CCNP R+S, CCNP Security- Dec 19, 2010. The Cisco Learning Network.*(11)

[12] S. Frankel, P. Hoffman, A. Nebaugh, R. Park., Guide to SSL VPNs, *National Institute of Standards and Technology U.S. Department of Commerce, July 2008.* (12)

[13] J. Guichard and I. Pepelnjah, MPLS/VPN Architecture Overview, *Case study: Virtual Private Networks in Supercom Provider Network, Aug 2, 2002, CISCO Press.* (13)

[14] A. Mason, Network Security and Virtual Private Network Technologies, *2014 Pearson Education, CISCO Press.*(14)

[15] R. Joyce, Virtual Private Networks, *Computer Science/Software Engineering, University Wisconsin-Platteville, 03 November 2007* (15)

[16] J. Doyle, Report 9: January 2013. Securing the JUSTIN system: Access and Security Audit at the Ministry of Justice, www.bcauditor.com, Office of the Auditor General of British Columbia, MACC, FCA. (16)

[17] Ministry of Justice, Republic of Macedonia, Ministry of Justice, Strategy for Justice Information Communication Technology 2007-2010, *Skopje, July 2007, Version 4.0* (17)

[18] Microsoft, Argentina's Ministry of Justice and Human Rights federal Agency Boosts Productivity by 40 Percent with Unified Communications Solution. *Microsoft Case Study: Microsoft Lync Server, 2010-Argentina's Ministry of Justice and Human Rights, 2014*(18)

[19] Republic of Austria, Use of IT within Austrian Justice, *Federal Ministry of Justice, eJustice, Austria, 2014, BMF* (19)

[20] USAID, ICT Country profile Georgia, 2013, *Regional Competitiveness initiative, ESI Center Eastern Europe* (20)

[21] Republic of Turkey, Department of information technologies and use of information technologies in the judiciary, *Ministry of Justice*. (21)

[22] Virtual Private Networking: An Overview, Sept, 2001, Microsoft:http://technet.microsoft.com/en-us/library/bb742566.aspx accessed 01/June/2014 (22)

[23] R.D.Doverspike, K.K. Ramakrishnan, C.Chase, *Chapter 2. Structural Overview of ISP Networks*, C.R. Kalmanek et al. (eds.), Guide to Reliable Internet Services and Applications,Computer Communications and Networks, DOI 10.1007/978-1-84882-828-5 2, Springer-Verlag London Limited 2010 (23).

[24] L.Todd, *Chapter 16: Cisco Certified Network Associate Deluxe Study Guide*, Sixth Edition, Sybex © 2011 Books 24 x7. (24)

[25] R. Joyce, *Virtual Private Networks*, Computer Science/Software Engineering, University Wisconsin-Platteville, 03 November 2007 (25)

[26] R.Graziani, A.Johnson, *Routing Protocols and Concepts, CCNA Exploration Companion Guide, Cisco Press, 2008 (26)*

[27] Vickygssn, *Network Protocols Handbook, 2nd edition, 2004-2005, Pg.(92-96, 106-109, 110-117)* (27)